IN THE CLAIMS:

1-24. **(Canceled)**

25. **(Currently Amended)** A method for operating a gaming machine comprising the steps of:

running an operating system loaded in the gaming machine;

providing and installing a trusted verification driver in the gaming machine, the trusted verification driver being independent of the operating system;

performing a verification of components of the operating system against a trusted reference using the trusted verification driver and preventing further operation of the gaming machine when the verification of the components of the operating system fails;

downloading at least one software module into the gaming machine;

checking a code signature of at least one downloaded software module using ~~a~~ **the** trusted verification driver, and

authorizing execution of the downloaded software module in the gaming machine only if the downloaded software module is successfully verified by the trusted verification driver.

26. **(Original)** The method of claim 25, wherein the running step runs an operating system that is configured to prevent a replacement of selected monitored or protected system files within the gaming machine with files that do not originate from a trusted source.

27. **(Original)** The method of claim 25, wherein the running step runs an operating system that is configured to prevent the execution of selected monitored or protected system files within the gaming machine for files that do not originate from a trusted source.

28. **(Currently Amended)** The method of claim 25, wherein the running step runs an operating system whose capability includes one of Microsoft's System File Protection (SFP) and ~~**Microsoft's**~~ Windows File Protection (WFP) **of the Microsoft Windows® operating system**.

29. **(Original)** The method of claim 25, wherein the operating system in the running step causes the authorizing step to authorize execution of the downloaded software module only if the downloaded software module has been code-signed with a certificate from a trusted source.

30. **(Currently Amended)** The method of claim 29, wherein the running step runs an operating system that includes ~~**Microsoft's**~~ Driver Signing **of the Microsoft Windows® operating system** and wherein the trusted source is Microsoft.

31. **(Currently Amended)** The method of claim 29, wherein the running step runs an operating system that includes ~~**Microsoft's**~~ Driver Signing **of the Microsoft Windows® operating system**.

32. **(Currently Amended)** The method of claim 30, wherein the downloaded software module includes a driver and wherein the method further comprises the step of:

setting a ~~**Microsoft**~~ Driver Signing policy **of the Microsoft Windows® operating system** to cause the authorizing step to only authorize execution of drivers that are code-signed with a certificate from one of Microsoft and a trusted source.

33. **(Currently Amended)** The method of claim 25, further comprising the step of:

setting a ~~Microsoft~~ Driver Signing policy **of the Microsoft Windows® operating system**,

and authorizing the installation and execution of the trusted verification driver subsequent to verifying that it is code-signed with a certificate from a trusted source.

34. **(Currently Amended)** The method of claim ~~32a~~ **33**, wherein the trusted source is Microsoft.

35. **(Currently Amended)** The method of claim ~~30a~~ **33**, further comprising the step of:

setting a ~~Microsoft~~ Driver Signing policy **of the Microsoft Windows® operating system** to cause the authorizing step to only authorize execution of drivers that are code-signed with a certificate from at least one of Microsoft and a designated trusted source.

36. **(Currently Amended)** The method of claim 25, wherein the operating system in the running step is a Microsoft Windows operating system configured with Software Restriction Policy, Windows File Protection and Driver Signing **of the Microsoft Windows® operating system.**

37-39. **(Canceled)**

40. **(Original)** The method of claim 25, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements capabilities specified by the Trusted Computing Platform Alliance (TCPA).

41. **(Original)** The method of claim 40, wherein the operating system in the running step is a Microsoft operating system.

42. **(Currently Amended)** The method of claim 25, wherein the operating system in the running step is ~~a Microsoft~~ **an** operating system implementing TCPA, Software Restriction Policy, Windows File Protection and Driver Signing **of the Microsoft Windows® operating system**.

43. **(Currently Amended)** The method of claim 25, wherein the operating system in the running step is a Microsoft Windows operating system configured with Software Restriction Policy, Windows File Protection and Driver Signing **of the Microsoft Windows® operating system** and wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements the Trusted Computing Platform Alliance (TCPA) specification.

44-46. **(Canceled)**

47. **(Currently Amended)** A method for verifying gaming terminal software, comprising the steps of:

installing at least one driver into the gaming machine;

blocking execution of an operating system of the gaming machine;

taking complete control of the gaming machine with the at least one driver;

verifying a legitimacy of all software and memory content in the gaming machine **using the at least one driver**;

relinquishing control of the gaming machine **back to the operating system**, and

authorizing the gaming machine to execute only ~~of the~~ software that is successfully verified.

48. **(Original)** The method of claim 47, whereby the at least one driver is configured to execute at a highest machine permission level.

49. **(Original)** The method of claim 47, wherein the taking step includes a step of freezing an operation of the operating system.

50. **(Canceled)** The method of claim 47, wherein the taking step includes a step of blocking the execution of the operating system.

51. **(Original)** The method of claim 47, wherein the taking step includes a step of disabling interrupts on the gaming machine.

52. **(Original)** The method of claim 47, wherein the verifying step includes verifying a BIOS of a motherboard of the gaming machine.

53. **(Original)** The method of claim 47, wherein the verifying step includes verifying a BIOS of any add-on board within the gaming machine.

54. **(Original)** The method of claim 47, wherein the verifying step includes verifying ROM shadowing within the gaming machine.

55. **(Original)** The method of claim 47, wherein the verifying step includes verifying hardware registers.

56. **(Original)** The method of claim 47, wherein the verifying step includes verifying a signature in memory of the at least one driver.

57. **(Original)** The method of claim 47, wherein the verifying step includes verifying a content of files on disk within the gaming machine.

58. **(Original)** The method of claim 47, wherein the verifying step includes verifying a downloadable micro-code of smart hardware within the gaming machine.

59. **(Original)** The method of claim 47, wherein the verifying step includes verifying a downloadable firmware of a smart hardware within the gaming machine.

60. **(Original)** The method of claim 47, further comprising the step of auditing a source code of the at least one driver by a third party.

61. **(Original)** The method of claim 47, further comprising the step of auditing a source code of the at least one driver by a game certification lab.

62. **(Original)** The method of claim 47, further comprising the step of certifying the at least one driver by a game certification lab.

63. **(Original)** The method of claim 47, further comprising the step of code-signing with a certificate the at least one driver by a game certification lab.

64. **(Original)** The method of claim 47, further comprising the step of certifying the at least one driver by a third party.

65. **(Original)** The method of claim 47, further comprising the step of code-signing with a certificate the at least one driver by a third party.

66. **(Original)** The method of claim 47, wherein the gaming machine is controlled by a PC, wherein the at least one driver is code signed and wherein the installing step installs the code-signed driver, the installing step being triggered by at least one plug-and-play dongle inserted in at least one port of the PC.

67. **(Canceled)**

68. **(Original)** The method of claim 47, wherein the verifying step verifies the legitimacy of the software and memory contents without modifying a content thereof and wherein the method further includes a step of reporting an outcome of the verifying step.

69. **(Currently Amended)** The method of claim 47, wherein the verification step includes a challenge-response step to ensure that the ~~**trusted verifier**~~ **at least one** driver has not been spoofed.

70. **(Currently Amended)** The method of claim 47, wherein the verification step includes a challenge-response step to ensure that the ~~**trusted verifier**~~ **at least one** driver is executing.

71. **(Original)** The method of claim 47, wherein the gaming machine further includes a third party dongle installed therein and wherein the at least one driver is linked to the third party dongle to enable the third party to audit the at least one driver.

72. **(Currently Amended)** The method of claim 47, wherein the gaming machine further includes an interface for a dongle compliant with ~~**the Microsoft**~~ **a** plug and play specification **of the Microsoft Windows® operating system** and wherein the at least one driver is installed or activated when the dongle is plugged-in.

73. **(Original)** The method of claim 47, wherein the gaming machine further includes a hard disk drive that includes at least one partition formatted for simple file access and wherein the method further includes a step of accessing code-signed downloaded software from the at least one simple file access partitioned hard disk drive.

74. **(Original)** The method of claim 73, wherein the hard disk drive partition is formatted according to FAT32 protocol.

75. **(Original)** The method of claim 73, wherein the hard disk drive partition is formatted according to a predetermined file format protocol.

76. **(Original)** The method of claim 47, wherein the gaming machine further includes a plurality of hard disk drives wherein at least one hard disk drive contains at least one partition formatted for simple file access and wherein the method further includes a step of accessing code-signed downloaded software from the at least one partition formatted for simple file access.

77. **(Original)** The method of claim 73, wherein the at least one partition is formatted according to FAT32 protocol.

78. **(Original)** The method of claim 73, wherein the at least one partition is formatted according to a predetermined file format protocol.

79. **(Original)** The method of claim 47, wherein the verifying step verifies the memory content or a trusted signature of the memory content stored on at least one of:

a hard disk drive of the gaming machine,

an optical memory of the gaming machine,

flash memory of the gaming machine,

non-volatile RAM memory of the gaming machine,

registers of integrated circuits of the gaming machine,

ferromagnetic memory of the gaming machine,

magnetic memory of the gaming machine,

ROM memory of the gaming machine,

OTP memory of the gaming machine,

holographic memory of the gaming machine, and

firmware of a smart peripheral.

80. **(Currently Amended)** A gaming machine, comprising:

at least one processor;

at least one data storage device;

a plurality of processes spawned by the at least one processor, the processes including processing logic for carrying out steps of:

running an operating system loaded in the gaming machine;

providing and installing a trusted verification driver in the gaming machine, the trusted verification driver being independent of the operating system;

performing a verification of components of the operating system against a trusted reference using the trusted verification driver and preventing further operation of the gaming machine when the verification of the components of the operating system fails;

downloading at least one software module into the gaming machine;

checking a code signature of at least one downloaded software module using ~~a~~ **the** trusted verification driver, and

authorizing execution of the downloaded software module in the gaming machine only if the downloaded software module is successfully verified by the trusted verification driver.

81. **(Original)** The gaming machine of claim 80, wherein the running step runs an operating system that is configured to prevent a replacement of selected monitored or protected system files within the gaming machine with files that do not originate from a trusted source or that are not consistent with the authorized version of the operating system.

82. **(Currently Amended)** The gaming machine of claim 80, wherein the running step runs a Microsoft operating system configured with a File Protection (WFP) **of the Microsoft Windows® operating system**.

83. **(Original)** The gaming machine of claim 80, wherein the operating system in the running step causes the authorizing step to authorize execution of the downloaded software module only if the downloaded software module has been code-signed with a certificate from a trusted source.

84. **(Currently Amended)** The gaming machine of claim 83, wherein the running step runs a Microsoft operating system configured with Driver Signing **of the Microsoft Windows® operating system** and wherein the trusted source is Microsoft.

85. **(Currently Amended)** The gaming machine of claim 83, wherein the running step runs a Microsoft operating system configured with Driver Signing **of the Microsoft Windows® operating system**.

86. **(Currently Amended)** The gaming machine of claim 80, wherein the downloaded software module includes a driver and wherein the method further comprises the step of:

setting a ~~Microsoft~~ Driver Signing policy **of the Microsoft Windows® operating system** to cause the authorizing step to only authorize execution of drivers that are code-signed with a certificate from Microsoft.

87. **(Currently Amended)** The method of claim 84, further comprising the step of:

setting a ~~Microsoft~~ Driver Signing policy **of the Microsoft Windows® operating system** to cause the authorizing step to only authorize execution of drivers that are code-signed with a certificate from at least one of Microsoft and a designated trusted source.

88. **(Currently Amended)** The gaming machine of claim 80, wherein the operating system in the running step is ~~a Microsoft Windows~~ **an** operating system configured with Windows File Protection and Driver Signing **of the Microsoft Windows® operating system**.

89. **(Currently Amended)** The gaming machine of claim 80, wherein the operating system in the running step is ~~a Microsoft Windows~~ **an** operating system configured with Software Restriction Policy, Windows File Protection and Driver Signing **of the Microsoft Windows® operating system**.

90-93. **(Canceled)**

94. **(Original)** The gaming machine of claim 80, wherein the gaming machine includes a processing hardware that, together with the operating system in the running step, implements capabilities specified by the Trusted Computing Platform Alliance (TCPA).

95. **(Currently Amended)** The gaming machine of claim 80, wherein the gaming machine includes a processing hardware that, together with the operating system in the

running step, implements capabilities specified by the Trusted Computing Platform Alliance (TCPA), Software Restriction Policy, System File Protection and Driver Signing **of the Microsoft Windows® operating system**.

96. **(Currently Amended)** The gaming machine of claim 80, wherein the gaming machine includes a processing hardware that, together with a Microsoft operating system in the running step, implements capabilities specified by the Trusted Computing Platform Alliance (TCPA), Software Restriction Policy, Windows File Protection and Driver Signing **of the Microsoft Windows® operating system**.

97. **(Original)** The gaming machine of claim 94, wherein the operating system in the running step is a Microsoft operating system.

98. **(Currently Amended)** The gaming machine of claim 80, wherein the operating system in the running step is ~~**a Microsoft**~~ **an** operating system implementing TCPA, Software Restriction Policies, Windows File Protection and Driver Signing **of the Microsoft Windows® operating system**.

99. **(Currently Amended)** The gaming machine of claim 80, wherein the operating system in the running step is ~~**a Microsoft**~~ **an** operating system implementing TCPA, Windows File Protection and Driver Signing Signing **of the Microsoft Windows® operating system**.

100. **(Currently Amended)** The gaming machine of claim 80, wherein the operating system in the running step includes the Software Restriction Policy capability Signing **of the Microsoft Windows® operating system**.

101. **(Currently Amended)** A gaming machine, comprising:

at least one processor;

at least one data storage device;

a plurality of processes spawned by the at least one processor, the processes including processing logic for carrying out steps of:

installing at least one driver into the gaming machine;

blocking the operation of an operating system of the gaming machine;

taking complete control of the gaming machine with the at least one driver;

verifying a legitimacy of all software and memory content in the gaming machine;

relinquishing control of the gaming machine **back to the operating system**, and

authorizing the gaming machine to execute only of the software that is successfully verified.

102. **(Original)** The gaming machine of claim 101, whereby the at least one driver is configured to execute at a highest machine permission level.

103. **(Original)** The gaming machine of claim 101, wherein the taking step includes a step of freezing an operation of the operating system.

104. **(Canceled)**

105. **(Original)** The gaming machine of claim 101, wherein the taking step includes a step of disabling interrupts on the gaming machine.

106. **(Original)** The gaming machine of claim 101, wherein the verifying step includes verifying a BIOS of a motherboard of the gaming machine.

107. **(Original)** The gaming machine of claim 101, wherein the verifying step includes verifying a BIOS of any add-on board within the gaming machine.

108. **(Original)** The gaming machine of claim 101, wherein the verifying step includes verifying ROM shadowing within the gaming machine.

109. **(Original)** The gaming machine of claim 101, wherein the verifying step includes verifying hardware registers.

110. **(Original)** The gaming machine of claim 101, wherein the verifying step includes verifying a signature in memory of the at least one driver.

111. **(Original)** The gaming machine of claim 101, wherein the verifying step includes verifying a content of files on disk within the gaming machine.

112. **(Original)** The gaming machine of claim 101, wherein the verifying step includes verifying a downloadable micro-code of smart hardware within the gaming machine.

113. **(Original)** The gaming machine of claim 101, wherein the verifying step includes verifying a downloadable firmware of a smart hardware within the gaming machine.

114. **(Original)** The gaming machine of claim 101, further comprising the step of auditing a source code of the at least one driver by a third party.

115. **(Original)** The gaming machine of claim 101, further comprising the step of auditing a source code of the at least one driver by a game certification lab.

116. **(Original)** The gaming machine of claim 101, further comprising the step of certifying the at least one driver by a game certification lab.

117. **(Original)** The gaming machine of claim 101, further comprising the step of code-signing with a certificate the at least one driver by a game certification lab.

118. **(Original)** The gaming machine of claim 101, further comprising the step of certifying the at least one driver by a third party.

119. **(Original)** The gaming machine of claim 101, further comprising the step of code-signing with a certificate the at least one driver by a third party.

120. **(Original)** The gaming machine of claim 101, wherein the processing hardware forms part of a PC that is configured to control the gaming machine and wherein the gaming machine further includes a plug and play dongle inserted in at least one port of the PC, and wherein the at least one driver is code signed and wherein the installing step installs the code-signed driver, the installing step being triggered by the at least one plug-and-play dongle.

121. **(Canceled)**

122. **(Original)** The gaming machine of claim 101, wherein the verifying step verifies the legitimacy of the software and memory contents without modifying a content thereof and wherein the plurality of processes include a process to report an outcome of the verifying step.

123. **(Currently Amended)** The method of claim 101, wherein the verification step includes a challenge-response step to ensure that the ~~**trusted verifier**~~ **at least one** driver has not been spoofed.

124. **(Currently Amended)** The method of claim 101, wherein the verification step includes a challenge-response step to ensure that the ~~**trusted verifier**~~ **at least one** driver is executing.

125. **(Original)** The gaming machine of claim 101, wherein the gaming machine further includes a third party dongle installed therein and wherein the at least one driver is linked to the third party dongle to enable the third party to audit the at least one driver.

126. **(Currently Amended)** The gaming machine of claim 101, wherein the gaming machine further includes an interface for a dongle compliant with ~~**the Microsoft**~~ **a** plug and play specification Signing **of the Microsoft Windows® operating system** and wherein the at least one driver is installed or activated when the dongle is plugged-in.

127. **(Original)** The gaming machine of claim 101, wherein the gaming machine further includes a hard disk drive that includes at least one a partition formatted for simple file access and wherein the plurality of processes include a process to access code-signed downloaded software from the at least one simple file access partitioned hard disk drive.

128. **(Original)** The gaming machine of claim 127, wherein the hard disk drive partition is formatted according to FAT32 protocol.

129. **(Original)** The gaming machine of claim 127, wherein the hard disk drive partition is formatted according to a predetermined file format protocol.

130. **(Original)** The gaming machine of claim 101, wherein the gaming machine further includes a plurality of hard disk drives wherein at least one hard disk drive contains at least one partition formatted for simple file access and wherein the method further includes a step of accessing code-signed downloaded software from the at least one partition formatted for simple file access.

131. **(Original)** The gaming machine of claim 128b, wherein the at least one partition is formatted according to FAT32 protocol.

132. **(Original)** The gaming machine of claim 128b, wherein the at least one partition is formatted according to a predetermined file format protocol.

133. **(Original)** The gaming machine of claim 101, wherein the verifying step verifies the memory content or a trusted signature of the memory content stored on at least one of:

a hard disk drive of the gaming machine,

an optical memory of the gaming machine,

flash memory of the gaming machine,

non-volatile RAM memory of the gaming machine,

registers of integrated circuits of the gaming machine,

ferromagnetic memory of the gaming machine,

magnetic memory of the gaming machine,

ROM memory of the gaming machine,

OTP memory of the gaming machine,

holographic memory of the gaming machine, and

firmware of a smart peripheral.

134-142. **(Canceled)**